

[shibboleth@nerisc.gov](mailto:shibboleth@nerisc.gov)

Steve Chan  
[sychan@lbl.gov](mailto:sychan@lbl.gov)



National Energy Research  
Scientific Computing Center



Lawrence Berkeley  
National Laboratory



## Intro

- **What?**
  - What is Shib?
  - What has been Shib-Enabled?
- **Why?**
  - What problem is solved?
  - Why should I care?
- **Who? Where?**
  - Who is using it?



# What is Shibboleth?

## Gratuitous Biblical Exegesis:

*The Gileadites captured the fords of the Jordan leading to Ephraim, and whenever a survivor of Ephraim said, "Let me cross over," the men of Gilead asked him, "Are you an Ephraimite?" If he replied, "No," they said, "All right, say 'Shibboleth.'" If he said, "Sibboleth," because he could not pronounce the word correctly, they seized him and killed him at the fords of the Jordan. Forty-two thousand Ephraimites were killed at that time.*

-Judges 12:5-6



# What is Shibboleth?

## Gratuitous Biblical Exegesis:

*The Gileadites captured the fords of the Jordan leading to Ephraim, and whenever a survivor of Ephraim said, "Let me cross over," the men of Gilead asked him, "Are you an Ephraimite?" If he replied, "No," they said, "All right, say 'Shibboleth.'" If he said, "Sibboleth," because he could not pronounce the word correctly, they seized him and killed him at the fords of the Jordan. Forty-two thousand Ephraimites were killed at that time.*

-Judges 12:5-6

## Ethnic Cleansing is in violation of LBL RPM section 7.01 ES&H:

### A. Policy

*It is the policy of Lawrence Berkeley National Laboratory to perform all work safely and with full regard to the well-being of workers, guests, the public, and the environment.*

*Keys to implementing this policy are the following core safety values:*

*[...]*

*Individuals demonstrate an awareness and concern for the safety of others.*

*Fatal Shibboleth Login failures are a STOP WORK situation!*



# What is Shibboleth?

## Shibboleth®

The Shibboleth System is a standards based, open source software package for web single sign-on across or within organizational boundaries. It allows sites to make informed authorization decisions for individual access of protected online resources in a privacy-preserving manner.

The Shibboleth software implements widely used federated identity standards, principally OASIS' Security Assertion Markup Language (SAML), to provide a federated single sign-on and attribute exchange framework. Shibboleth also provides extended privacy functionality allowing the browser user and their home site to control the attributes released to each application. Using Shibboleth-enabled access simplifies management of identity and permissions for organizations supporting users and applications. Shibboleth is developed in an open and participatory environment, is freely available, and is released under the Apache Software License.

From: <http://shibboleth.internet2.edu/about.html>



# What is Shibboleth?

## SAML – Security Assertion Markup Language

Standard XML schemas for exchanging security and identity information and HTTP based protocols for passing XML messages back and forth



# What is Shibboleth?

## SAML – Security Assertion Markup Language

Standard XML schemas for exchanging security and identity information and HTTP based protocols for passing XML messages back and forth

### Attributes

Assertions about a user(principal) such as user id, name, organizational affiliation/roles. Much of it based on common x509/LDAP attributes. Attributes are encoded and transmitted in SAML



# What is Shibboleth?

## SAML – Security Assertion Markup Language

Standard XML schemas for exchanging security and identity information and HTTP based protocols for passing XML messages back and forth

## Attributes

Assertions about a user(principal) such as user id, name, organizational affiliation/roles. Much of it based on common x509/LDAP attributes. Attributes are encoded and transmitted in SAML

## Federation

Metadata standards supporting trust relationships to enable Federated Login



# What is Shibboleth?

## SAML – Security Assertion Markup Language

Standard XML schemas for exchanging security and identity information and HTTP based protocols for passing XML messages back and forth

## Attributes

Assertions about a user(principal) such as user id, name, organizational affiliation/roles. Much of it based on common x509/LDAP attributes. Attributes are encoded and transmitted in SAML

## Federation

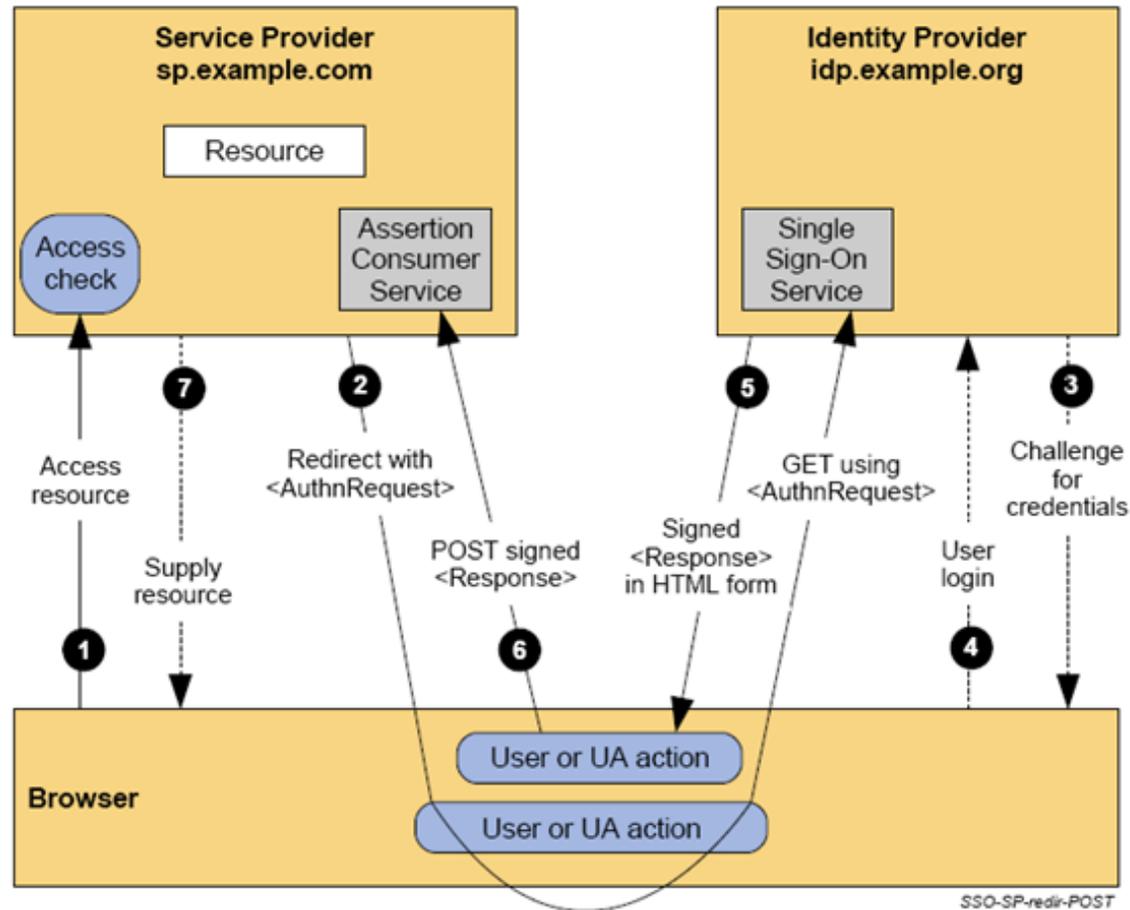
Metadata standards supporting trust relationships to enable Federated Login

## Shibboleth/SAML

Shibboleth provides conventions for attributes, standards around metadata discovery and exchange, and policy controls to support privacy and other organizational goals to support the Research and Education community. Shibboleth 2.0 and SAML 2.0 converge on metadata standards

# What is Shibboleth?

## Shibboleth Web Login transaction



From: [http://wiki.eclipse.org/SAML2\\_IdP](http://wiki.eclipse.org/SAML2_IdP)



# Why Single Sign On?

## Pro:

**Reduces “password fatigue” from too many different passwords**

**Sensitive/Secure information is centralized and less exposed**

example: the web server gets compromised and used to harvest creds

**Fewer locations where passwords are maintained**

**Convenience avoids possibly insecure workarounds by users**

example: having the browser cache passwords

**Centralized audit location**

## Con:

**Training**

User is now logged into everything, and logout is more complex

Admins have to learn new technology

**Single point of failure**



# What is using shib at NERSC?

## shib.nersc.gov is the Identity Provider (IdP)



Please login below with your NIM username and password to access pages with personalized information and NERSC user-only content.

USERNAME:

PASSWORD:

Login

All NERSC users have NIM accounts. If you do not know your NIM password, please contact the NERSC Account Support office at 1-800-66-NERSC (510-486-6800), menu option 2. Please report all web login problems to [webmaster@nersc.gov](mailto:webmaster@nersc.gov) or the NERSC consultants at 1-800-66-NERSC, menu option 3.

A U.S. Department of Energy User Facility at Lawrence Berkeley National Laboratory



QUESTIONS & COMMENTS





# What is using shib at NERSC?

Communicates with LDAP, handles all credentials, returns attributes



Please login below with your NIM username and password to access pages with personalized information and NERSC user-only content.

USERNAME:

PASSWORD:

Login

All NERSC users have NIM accounts. If you do not know your NIM password, please contact the NERSC Account Support office at 1-800-66-NERSC (510-486-6800), menu option 2. Please report all web login problems to webmaster@nersc.gov or the NERSC consultants at 1-800-66-NERSC, menu option 3.

A U.S. Department of Energy User Facility at Lawrence Berkeley National Laboratory



QUESTIONS & COMMENTS



U.S. DEPARTMENT OF  
**ENERGY**

Office of  
Science





# What is using shib at NERSC?

[www.nersc.gov](http://www.nersc.gov) is a Service Provider (SP)

The screenshot shows the NERSC website homepage. At the top left is the NERSC logo with the tagline "Powering Scientific Discovery Since 1974". To the right is a search bar and a "My NERSC | Site Map | Share" link. Below the logo is a navigation menu with items: HOME, ABOUT, SYSTEMS, FOR USERS, SCIENCE AT NERSC, NEWS & PUBLICATIONS, R & D, EVENTS, and LIVE STATUS. The main header reads "National Energy Research Scientific Computing Center". Below this is a large banner for "The MATERIALS PROJECT" featuring a woman's portrait and the text "a materials genome approach". A sidebar on the right of the banner says "ACCELERATING ADVANCED MATERIAL DEVELOPMENT" and "The Materials Project brings genome-like computing to the aid of scientists searching for the stuff to build better batteries, fuel cells and other energy-related products." Below the banner are two columns: "COMPUTING AT NERSC" with sub-links "OUR SYSTEMS", "GETTING STARTED", "DOCUMENTATION FOR USERS", and "LIVE STATUS"; and "ANNOUNCEMENTS" with items like "NERSC 2012 awards" and "Magellan Queues End November 30". At the bottom left of the screenshot is a "NOW COMPUTING" section with the text "A small sample of massively parallel scientific computing jobs running right now at NERSC."



Office of Science



Lawrence Berkeley National Laboratory



# What is using shib at NERSC?

Service Provider is a web application dependent on IdP for authentication

The screenshot shows the NERSC website homepage. At the top left is the NERSC logo with the tagline "Powering Scientific Discovery Since 1974". To the right is a search bar and links for "My NERSC", "Site Map", and "Share". A navigation menu includes "HOME", "ABOUT", "SYSTEMS", "FOR USERS", "SCIENCE AT NERSC", "NEWS & PUBLICATIONS", "R & D", "EVENTS", and "LIVE STATUS". The main banner features a woman's portrait and the text "The MATERIALS PROJECT" and "a materials genome approach". A text box on the banner reads: "ACCELERATING ADVANCED MATERIAL DEVELOPMENT. The Materials Project brings genome-like computing to the aid of scientists searching for the stuff to build better batteries, fuel cells and other energy-related products. > Read More". Below the banner are two columns: "COMPUTING AT NERSC" with sub-sections "OUR SYSTEMS", "GETTING STARTED", "DOCUMENTATION FOR USERS", and "LIVE STATUS"; and "ANNOUNCEMENTS" with items like "NERSC 2012 awards", "Magellan Queues End November 30", and "Bioinformatics Computing Consultant Position Available". At the bottom left of the screenshot, it says "A small sample of massively parallel scientific computing jobs running right now at NERSC."



Office of Science



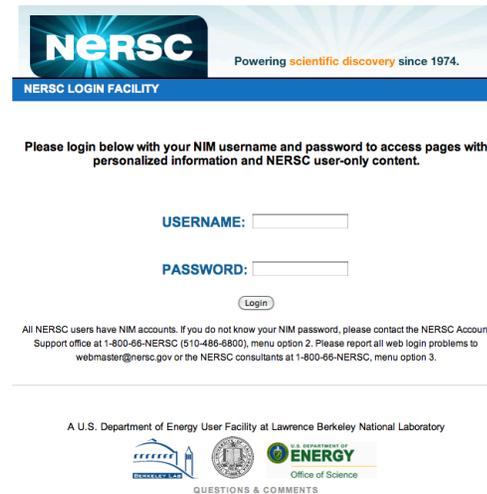
Lawrence Berkeley National Laboratory



# What is using shib at NERSC?

The Service Provider ([www.nersc.gov](http://www.nersc.gov)) requests authentication attributes from the Identity Provider ([shib.nersc.gov](http://shib.nersc.gov)).

Once these attributes are received, the business logic in the SP decides on authorization for the user.





# What is using shib at NERSC?

## ServiceNow

**NERSC** National Energy Research Scientific Computing Center

Welcome: Stephen Chan

Switch to the old UI

**Incident Overview**

**Priority 1 Incidents**

**Incident Summary Counts**

- Critical Incidents**: 1 (Open Incidents that have Critical priority)
- Overdue Incidents**: 0 (Open Incidents that have attained an overdue escalation value)
- Incidents Opened > 1 Week**: 13 (Incidents that have stayed open for longer than a week)

**Unassigned Incidents**

| Number     | Resource  | Category               | Title                              |
|------------|-----------|------------------------|------------------------------------|
| INC0010297 | Request   | Request                | accounts test                      |
| INC0010299 | Request   | Request                | .bash_profile doesn't work in HPSS |
| INC0010557 | PDSF      | Running Jobs           | Jobs don't run                     |
| INC0010588 | Archive   | Information Technology | This is a test.                    |
| INC0010591 | JGI       | Network                | This is a test #2.                 |
| INC0010595 | NERSC Web | Data/IO                | This is a test #3.                 |

**Open Incidents By State**

- New = 20 (51%)
- Active = 17 (44%)
- User Updated = 1 (3%)
- Active - Expectations Set = 1 (3%)

**Open Incidents By Category**

- Request = 7
- Miscellaneous = 5
- (empty) = 4
- Information Technology = 4
- Network = 4
- Account Support = 3
- Data/IO = 3
- Hardware = 3
- Running Jobs = 3
- Programming = 2
- Software = 1



# What additional features?

**Single Sign On** (currently disabled)

**JAAS Authentication handler** (stackable)

**Radius Authentication (otp for Web SSO)**

Possibly useful when traveling to Cyber-Mordor (aka China)

**Kerberos Authentication**

**LDAP**

**REMOTE\_USER authentication**

IdP looks for \$REMOTE\_USER for authentication

**Database backed attributes (JDBC)**



# Who else is using shib?

## Popular in R&E Communities:

**UC Trust:** UCB, UCLA, UCSD, UCD, UCM, UCSF, LBNL, UCI, UCR, UCSC, UCOP

**Major Research Universities:** Caltech, CMU, Columbia, Cornell, Duke, Georgetown, GA Tech, JHU, MIT, Princeton, Purdue, RPI, Stanford, U Chicago, UIUC, Penn, Yale, etc...

**Companies with strong .edu ties and research institutions:** Apple, CollegeNet, Internet2, NIH, Smithsonian, ANL, Globus, Teragrid, VOMS

**Software As Service Providers:** Google, Microsoft, Salesforce, Oracle, ServiceNow, IBM



# InCommon Federation

**InCommon.org is a large identity federation**

Approx. 360 members

Contains all of the members in previous slide

**Assurance Program**

**Certificate Service**

**NERSC is an affiliate**

**Provides a Discovery Service**

Login entry point for applications that makes available all the Identity Providers of members



# InCommon Federation

Select your School, Organization, or Identity Provider:

University of California, Berkeley

Do not remember my selection  
 Remember my selection for this session only  
 Remember my selection permanently

[About InCommon](#) [Help](#)

© Copyright 2011, InCommon, LLC | [incommon.org](http://incommon.org) | InCommon: Identity and Access for Research and Education



# InCommon Federation

Select your School

https://wayf.i

Google Status

- Rice University
- Rockingham County Schools
- Rutgers, The State University of New Jersey
- San Diego State University
- San Francisco State University
- San Jose State University
- Santa Barbara City College
- Smithsonian Institution
- Sonoma State University
- Stanford University
- Stark State College of Technology
- Stevens Institute of Technology
- Stony Brook University
- Texas A & M University
- Texas State University – San Marcos
- The State University of New York at Buffalo
- The University of Arizona
- The University of Findlay
- The University of Memphis
- Tulane University
- Unicon, Inc.
- University of Alabama at Birmingham
- University of Alaska Statewide System
- University of Arkansas Main Campus
- University of Arkansas for Medical Sciences
- University of Baltimore
- University of California – Office of the President
- ✓ University of California, Berkeley**
- University of California, Davis
- University of California, Merced
- University of California, Riverside
- University of California, San Francisco
- University of California, Santa Cruz
- University of California–Irvine
- University of California–Los Angeles
- University of California–San Diego
- University of California–Santa Barbara
- University of Central Florida
- University of Chicago
- University of Cincinnati Main Campus
- University of Dayton
- University of Delaware
- University of Florida
- University of Hawaii
- University of Houston–Downtown
- University of Illinois At Springfield

© Copyright 2011, InCommon

about InCommon | Help

and Access for Research and Education



U.S. DEPARTMENT OF  
**ENERGY**

Office of  
Science



Lawrence Berkeley  
National Laboratory



# Science Identity Federation

## DOE Specific Federation

Led by Mike Helm [M\\_Helm@lbl.gov](mailto:M_Helm@lbl.gov)

### Mailing List:

<http://groups.google.com/group/science>

Basic discovery service

Interesting service – [confluence.scifed.org](http://confluence.scifed.org)

Several test IDPs

Blanket contract for InCommon membership

Training Events (Shib Install Fest)

NERSC is a member



# What/Who else is Shib-Enabled?

## Shibboleth Wiki is good resource:

<https://wiki.shibboleth.net/confluence/display/SHIB2/ShibEnabled>

Elsevier Science Direct  
JSTOR  
American Chemical Society  
UC At Your Service Online  
Apples iTunes U

Apache Webserver

Blackboard  
Moodle  
Sakai

Confluence Wiki  
Drupal

Google Apps/Gmail  
GridSphere  
GridShib  
Joomla  
MediaWiki  
MoinMoin Wiki  
SYMPA  
Twiki  
Workpress  
Silverstripe  
ServiceNow

Oracle 10g/11g  
BEA/WebSphere



# Who/What *could* be ShibEnabled?

Web applications are easily ShibEnabled with Apache Shib Module

<https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPLinuxInstall>

Once module is configured, shibboleth login info is passed in via CGI environment variables available to PHP, CGI, etc...

|  |   |
|--|---|
| _SERVER["Shib-Session-ID"]             | _7a82077fcdd2b965d8118826c2bd9dfd                                 |
| _SERVER["Shib-Identity-Provider"]      | https://login.lbl.gov/idp/shibboleth                              |
| _SERVER["Shib-Authentication-Instant"] | 2011-12-14T23:11:09.137Z  |
| _SERVER["Shib-Authentication-Method"]  | urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport |
| _SERVER["Shib-AuthnContext-Class"]     | urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport |
| _SERVER["Shib-Session-Index"]          | 63c5159b8880ffaa8b4ed85992379d11b8bb35627d1a75c893d5c30dcc0d01f2  |
| _SERVER["Shib-affiliation"]            | Staff@lbl.gov;Member@lbl.gov                                      |
| _SERVER["Shib-cn"]                     | Steve Chan;Stephen Chan   |
| _SERVER["Shib-displayName"]            | Chan, Stephen (Steve)   |
| _SERVER["Shib-employeeNumber"]         | 004285  |
| _SERVER["Shib-entitlement"]            | lblUser   |
| _SERVER["Shib-eppn"]                   | SYChan@lbl.gov  |
| _SERVER["Shib-givenName"]              | Stephen   |
| _SERVER["Shib-mail"]                   | SYChan@lbl.gov  |
| _SERVER["Shib-sn"]                     | Chan  |
| _SERVER["Shib-uid"]                    | SYChan  |



# Multidomain Login Demo

**Demo Wordpress instance at:**

<https://webdev1.nersc.gov/~sychan/wpdemo/>

**WordPress 3.3**

<http://wordpress.org/download/>

**Shib Module 1.4:**

<http://wordpress.org/extend/plugins/shibboleth/>

**Apache 2.2 and Shibboleth NativeSP**

**Customized Login Page**



# Multidomain Login Demo

## Apache directives for shib:

```
<Location /~sychan/>  
  AuthType shibboleth  
  ShibRequireSession Off  
  require shibboleth  
</Location>
```

## Significant config directives for shibd – back end to apache module. Documented at:

<https://sites.google.com/a/lbl.gov/csd-silverstripe/web-administrator/shibboleth-sp-configuration/apache-nativesp>

## Shibboleth uses lots and lots of XML – bring XML allergy meds

You are in a maze of twisty little XML stanzas, all alike



# Multidomain Login Demo

## Login Domain Director Page logindemo.php:

```
<?php

echo "<center>Test login from the following authentication domains:<br/><br/><br/>";

echo '<a href="https://webdev.nersc.gov/Shibboleth.sso/Login?entityID=https%3A//login.lbl.gov/idp/shibboleth&' . $_SERVER['QUERY_STRING'] . '"></a><br/><br/><br/>';

echo '<a href="https://webdev.nersc.gov/Shibboleth.sso/Login?entityID=https%3A//shib.nersc.gov/idp/shibboleth&' . $_SERVER['QUERY_STRING'] . '"></a><br/><br/><br/><br/>';

echo '<a href="https://webdev.nersc.gov/Shibboleth.sso/Login?entityID=https%3A//shib.nersc.gov/idp/JGI/shibboleth&' . $_SERVER['QUERY_STRING'] . '"></a><br/>';

echo "</center>";

?>
```



# Questions? Brainstorming

**Do we have users that want to access resources at NERSC, but don't have NIM accounts?**

**Are there applications at other sites that NERSC users want to access without getting account at remote site?**

**Are there applications where we want groups from multiple sites to have access too, without consolidating user db?**

**Do we want to allow some form of NERSC authentication on hosts that we don't really trust, or on remote networks where LDAP access would be undesirable?**